An Initiative of CollCom

Empowering Youth through Community Service

ISSN: 2583-9969

Vol 17, Issue May 2024

CYBER संस्कार

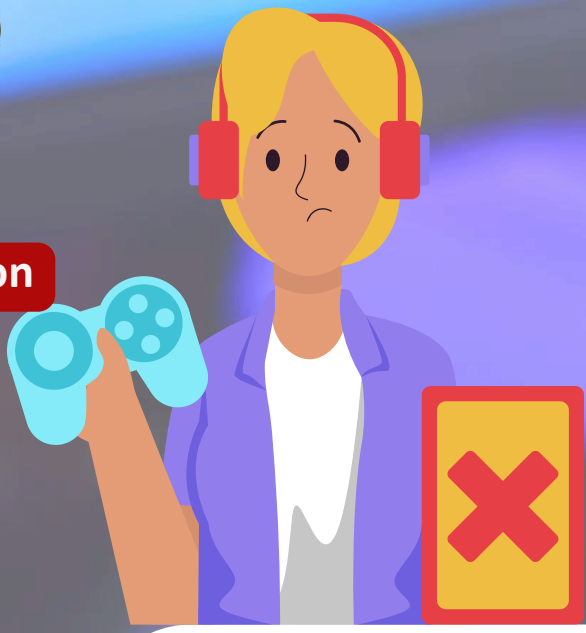
साइबर अपराध के खिलाफ एक कदम

Online Child Sexual Abuse

Parental control

Religion Conversion

Online Grooming



प्रीतेश मिश्रा

डॉ गौरव कुमार

Online Gaming Fraud !

साइबर संस्कार : Online Gaming Fraud!

प्रीतेश मिश्रा, डॉ गौरव कुमार

प्रकाशक : कॉलकम

1043/2, मेहरावाली अपार्टमेंट,
महरौली नई दिल्ली, 110030, भारत

संपर्क: +91 -9868189955

ईमेल: pr@collcom.org

वेबसाइट: www.collcom.org

प्रथम संस्करण : मई 2024

मूल्य : ₹ 49

मुद्रक : कॉलकम, भारत

ISSN : 2583-9969

Abstract (सार)

आज के डिजिटल युग में, भारत में ऑनलाइन गेमिंग का क्रेज तेजी से बढ़ रहा है। ऑनलाइन गेमिंग का मतलब इंटरनेट के जरिए खेले जाने वाले गेम्स से है। इसमें खिलाड़ी कंप्यूटर, मोबाइल, या कंसोल पर गेम्स खेलते हैं, जो कि दुनिया भर के अन्य खिलाड़ियों के साथ जुड़े होते हैं। ये गेम्स मनोरंजन के साथ-साथ बच्चों और युवाओं के लिए सीखने और एक-दूसरे के साथ जुड़ने, दोस्ती करने, सहयोग करने, या प्रतिस्पर्धा करने का अवसर प्रदान करती हैं। एक ओर यह उद्योग युवा पीढ़ी के लिए मनोरंजन का नया साधन बन गया है, वहीं दूसरी ओर साइबर अपराधियों के लिए एक नए शिकार स्थल के रूप में उभर रहा है।

एक 12 वर्षीय लड़की की कल्पना करें, जो हर दिन स्कूल के बाद एक घंटे तक ऑनलाइन गेम खेलती है। गेमिंग के दौरान, वह अन्य खिलाड़ियों के साथ चैट करती है और कभी-कभी अपनी गेमिंग का लाइवस्ट्रीम भी करती है। अक्सर, उसे यह नहीं पता होता कि स्क्रीन के दूसरी तरफ कौन है या वे कहाँ से हैं, लेकिन इससे उसे ज्यादा फर्क नहीं पड़ता। उसका पूरा ध्यान सिर्फ एक चीज़ पर है - खेल में सबसे बेहतरीन खिलाड़ी बनना! यह स्थिति कई बच्चों के लिए आम है, जो उन्हें उन अपराधियों का शिकार बना सकती है जो ऑनलाइन प्लेटफॉर्म का उपयोग करके उनका यौन शोषण करना चाहते हैं। इसके साथ ही, बच्चों को साइबरबुलिंग और अभद्र भाषा का भी सामना करना पड़ता है, जो उनके मानसिक और भावनात्मक स्वास्थ्य को गंभीर रूप से प्रभावित कर सकते हैं। ऐसे जोखिम बच्चों की सुरक्षा के लिए एक बड़ी चुनौती बन गए हैं, जिनसे निपटने के लिए जागरूकता और सतर्कता की जरूरत है।

2023 के वैश्विक खतरा आकलन (Global Threat Assessment) के अनुसार, ऑनलाइन बाल यौन शोषण और दुर्व्यवहार की घटनाएं दुनिया भर में तेजी से बढ़ रही है। नेशनल सेंटर फॉर मिसिंग एंड एक्सप्लॉइटेड चिल्ड्रन (NCMEC) द्वारा विश्लेषित रिपोर्ट्स के अनुसार, 2019 से 2023 तक बाल यौन शोषण सामग्री की रिपोर्ट में 87% की वृद्धि हुई है। अपराधी नए डिजिटल प्लेटफ़ॉर्म, जैसे कि गेमिंग ऐप्स, सोशल मीडिया, और लाइव स्ट्रीमिंग सर्विसेज़ का उपयोग करके अधिक गुप्त और जटिल तरीकों से बच्चों को निशाना बना रहे हैं। ये आंकड़े बताते हैं कि बच्चों के खिलाफ ऑनलाइन अपराधों में तेजी से वृद्धि हो रही है, जो वैश्विक स्तर पर एक गंभीर चिंता का विषय बन गई है।

अपराधी अक्सर नकली प्रोफाइल बनाकर बच्चों से दोस्ती करते हैं और अश्लील सामग्री साझा कर उन्हें ब्लैकमेल करते हैं। इसके अलावा, साइबरबुलिंग, नशा, गोपनीयता का खतरा, और वित्तीय धोखाधड़ी जैसी समस्याएं भी ऑनलाइन गेमिंग से जुड़ी हुई हैं। ये सभी चिंताएं बच्चों की सुरक्षा, मानसिक स्वास्थ्य और समय प्रबंधन पर नकारात्मक प्रभाव डाल सकती हैं, जिससे ऑनलाइन सुरक्षा के उपायों को अपनाना अनिवार्य हो जाता है।

यह पत्रिका ऑनलाइन गेमिंग घोटालों और सुरक्षा उपायों से संबंधित सभी मामलों को सामने लाने के लिए डिज़ाइन किया गया है। इसमें वास्तविक जीवन के विभिन्न उदाहरणों के माध्यम से बताया गया है कि कैसे अपराधी गेमिंग प्लेटफ़ॉर्म का उपयोग करके बच्चों और युवाओं को धोखा देते और शोषण करते हैं। इसका उद्देश्य पाठकों को इन खतरों के बारे में जागरूक करना और आवश्यक सुरक्षा उपाय अपनाने के लिए प्रेरित करना है, ताकि वे अपने और अपने बच्चों की ऑनलाइन सुरक्षा सुनिश्चित कर सकें।

विषय-सूची

Online Gaming Fraud !

Contents

callcom
Empowering Youth through Community Service

Page No.

ONLINE GAMING के जरिए ठगी का अंबार।

दैनिक भास्कर

भास्कर एक्सक्लूसिव ऑनलाइन गेमिंग में 500 जीते, फिर 7 करोड़ हारे: गेम खिलाने वाले बोले- फंसाते नहीं, लोग खुद फंसते, फिर मर जाते हैं

amarujala.com

अमर उजाला — एप डाउनलोड करें

AstraZeneca Vaccine | Indian Railway | Tri

Online Gaming Fraud Case: ढाई किलो सोना, 70 लाख की नकदी जब्त, गोंदिया में नागपुर पुलिस ने की छापेमारी

GADGETS NOW by THE TIMES OF INDIA — OPEN APP

NEWS VIDEOS CITY INDIA ELECTIONS

Online Gaming App Scam 'E-Nugget': ED Freezes Rs 90 Crore In 70 Accounts

| TOI Tech Desk | TIMESOFINDIA.COM | May 2, 2024, 07:16 IST

अमर उजाला — एप डाउनलोड करें

Online Gaming: सरकार ने बैन किए 581 गेमिंग एप, सरकार की साइबर टीम ने जारी किया अलर्ट

टेक डेस्क, अमर उजाला, नई दिल्ली Published by: प्रदीप पाण्डेय
Updated Wed, 24 Jan 2024 03:39 PM IST

g2g.news

Gaming

Woman loses Rs.1 Lakh in a fraud involving online gaming app, FIR filed

By TeamG2G - Modified date: March 22, 2024

thehindu.com

HOME / NEWS / CITIES / VISAKHAPATNAM

People conned of ₹9.58 crore in 'task game fraud' cases in Visakhapatnam this year, says Police Commissioner

aajtak.in

27 गेमिंग वेबसाइट, 6000 बैंक खाते और 15 लाख लोग.... पुलिस ने ऐसे बचाया यूपी का होने वाला सबसे बड़ा फ्रॉड

business-standard.com

Business Standard

Home Latest E-paper Markets Elect Subscribe

Sensex ↓ (-0.25%) 74482.78 -188.50 | Nifty ↓ (-0.17%) 22604.85 -38.55 | Nifty Mid 50868.20

Home / India News / Mahadev betting app case: Everythi

Mahadev betting app case: Everything known about the Rs 6k cr scam so far

news18.com

NEWS18 — LIVE TV — JOIN US

Home Latest Movies Elections 2024 IPL 2024

NEWS / INDIA / ONLINE GAMING FRAUD CASE: NAGPUR PO...

Online Gaming Fraud Case: Nagpur Police Seize 2.4 Kg Gold, Rs 70 Lakh Cash During Raids in Gondia

indiatoday.in

INDIA TODAY NORTHEAST MALAYALAM

INDIA TODAY — Magazine | Live TV | Search

Home / Technology / News / Online gaming scam involving...

Online gaming scam involving Rs 58 crore in Nagpur, if you game online use these tips to stay safe

ONLINE GAMING FRAUD!

आज हम आपको भारत में हो रहे गेमिंग फ्रॉड स्कैम्स की सच्चाई से अवगत कराएंगे और बताएंगे कि कैसे स्कैमर्स मासूम खिलाड़ियों को अपने जाल में फंसा लेते हैं। इस जानकारी को समझना न केवल हमारे लिए आवश्यक है, बल्कि यह समय की मांग भी है, ताकि हम सभी अपने और अपने प्रियजनों को इन धोखाधड़ियों से सुरक्षित रख सकें। आइए, जानें कि इन खतरनाक स्कैम्स से कैसे बचा जा सकता है और खुद को डिजिटल दुनिया में सुरक्षित कैसे रखा जा सकता है।

आज के डिजिटल युग में **ऑनलाइन गेमिंग का क्रेज तेजी** से बढ़ रहा है। जहां एक ओर यह उद्योग युवा पीढ़ी के लिए मनोरंजन का नया साधन बन गया है, वहीं दूसरी ओर साइबर अपराधियों के लिए एक नए शिकार स्थल के रूप में उभर रहा है।

गेमिंग की इस चमचमाती दुनिया के पीछे छिपे धोखाधड़ी और स्कैम ने न केवल खिलाड़ियों को आर्थिक नुकसान पहुँचाया है, बल्कि उनके व्यक्तिगत डेटा और गोपनीयता को भी गंभीर खतरे में डाल दिया है।

REPORT

फेडरेशन ऑफ इंडियन चैंबर्स ऑफ कॉमर्स एंड इंडस्ट्री की एक रिपोर्ट के अनुसार, भारत में ऑनलाइन गेमिंग में भुगतान करने वाले नए उपयोगकर्ताओं (NPU*) का अनुपात दुनिया में सबसे तेज गति से बढ़ा है। यह आंकड़ा **2020 में 40% था, जो 2021 में 50% और 2023 में बढ़कर 80%** तक पहुंच गया है।

***नए पेइंग यूजर्स (NPUs) वे खिलाड़ी होते हैं जो किसी ऑनलाइन गेमिंग प्लेटफॉर्म पर पहली बार पैसे खर्च करते हैं। ये यूजर्स गेमिंग कंपनियों के लिए विशेष रूप से महत्वपूर्ण होते हैं क्योंकि ये प्लेटफॉर्म की वित्तीय वृद्धि में योगदान करते हैं।**

लॉयड्स बैंक द्वारा किए गए एक अध्ययन के अनुसार, बच्चे पहले से कहीं अधिक समय ऑनलाइन गेम खेलने में बिता रहे हैं, **3 से 15 वर्ष की आयु** के बीच के **5 मिलियन से अधिक बच्चे** अब नियमित रूप से ऑनलाइन गेम खेल रहे हैं, जो 2019 की तुलना में लगभग 4.6 मिलियन से अधिक है। लॉयड्स के उसी अध्ययन से ये भी पता चला कि एक तिहाई (36%) से अधिक माता-पिता अपने बच्चों के गेमिंग धोखाधड़ी का शिकार होने और पैसे खोने की संभावना को लेकर काफी चिंतित हैं।

इन आंकड़ों से यह स्पष्ट होता है कि यह समस्या कितनी गंभीर है। अपने बच्चों के भविष्य को सुरक्षित रखने और इस तरह के फ्रॉड से बचने के लिए इसके विभिन्न पहलुओं को समझना बेहद आवश्यक हो जाता है। जागरूकता और सतर्कता ही हमें इस बढ़ते खतरे से बचा सकती है।

Online Gaming Fraud क्या है ?

ऑनलाइन गेमिंग फ्रॉड वह धोखाधड़ी है, जिसमें साइबर अपराधी ऑनलाइन गेमिंग प्लेटफ़ॉर्म का उपयोग करके खिलाड़ियों को ठगते हैं। यह फ्रॉड कई तरीकों से किया जा सकता है, जैसे कि फर्जी गेमिंग वेबसाइट्स, नकली इन-गेम आइटम्स की खरीद, फिशिंग लिंक के माध्यम से व्यक्तिगत जानकारी चुराना, बाल यौन शोषण या खिलाड़ियों के खातों को हैक करके उनके वित्तीय संसाधनों का दुरुपयोग करना। इन फ्रॉड्स का **मुख्य उद्देश्य खिलाड़ियों से पैसा और डेटा चोरी** करना होता है।

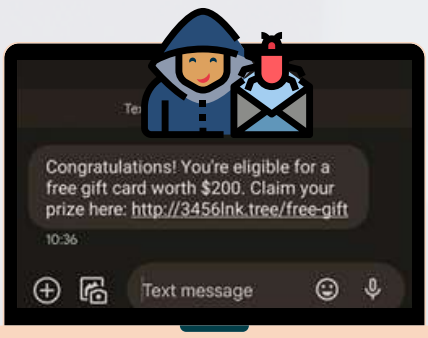
ऑनलाइन गेमिंग स्कैम्स में स्कैमर्स खिलाड़ियों को धोखा देने के लिए कई तरह के तरीके अपनाते हैं। आमतौर पर, ये स्कैमर्स **नकली गेमिंग प्लेटफ़ॉर्म्स, फर्जी वेबसाइट्स, ईमेल्स, और मैसेजेस** का उपयोग करते हैं ताकि खिलाड़ियों से उनकी लॉगिन जानकारी, बैंकिंग विवरण, और व्यक्तिगत डेटा चुरा सकें। इस प्रक्रिया को **फिशिंग** कहा जाता है, जहां वे विश्वसनीय स्रोतों का रूप धारण कर खिलाड़ियों को अपने जाल में फंसाते हैं।

फिशिंग के अलावा, स्कैमर्स न**कली इन-गेम आइटम्स की खरीदारी या शानदार बोनस और पुरस्कारों/करेंसी** के बहाने भी खिलाड़ियों से धन उगाही करने का प्रयास करते हैं।

- कुछ मामलों में, स्कैमर्स गेमिंग एप्लिकेशन या मोड्स में छिपे हुए मैलवेयर शामिल करते हैं, जो खिलाड़ियों के डिवाइस को संक्रमित कर उनकी संवेदनशील जानकारी चुरा सकते हैं। यह मैलवेयर न केवल डेटा को खतरे में डालता है, बल्कि डिवाइस के समग्र प्रदर्शन को भी प्रभावित करता है।
- इसके अलावा, स्कैमर्स **सामाजिक इंजीनियरिंग** का भी सहारा लेते हैं, जिसमें वे खेल के दौरान खिलाड़ियों से दोस्ती करके और उनका विश्वास जीतकर उनसे व्यक्तिगत जानकारी प्राप्त करने की कोशिश करते हैं। एक बार जब वे खिलाड़ियों का भरोसा हासिल कर लेते हैं, तो वे इस जानकारी का उपयोग धोखाधड़ी करने और वित्तीय या व्यक्तिगत नुकसान पहुंचाने के लिए करते हैं।

आइए, ऑनलाइन गेमिंग स्कैम्स कैसे काम करते हैं, इसे थोड़ा विस्तार से समझने का प्रयास करते हैं।

फिशिंग लिंक/ऐप स्कैम

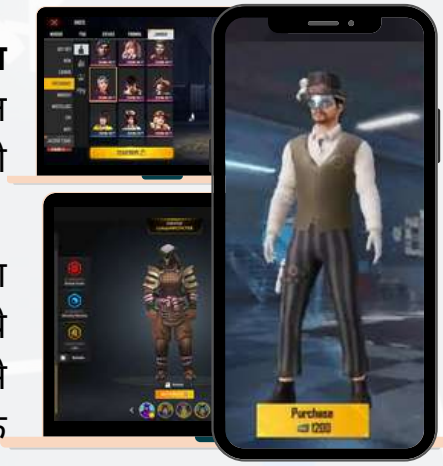


कैसे काम करता है: स्कैमर्स फर्जी ईमेल, मैसेज, या नकली वेबसाइट्स/ऐप्स का उपयोग करके खिलाड़ियों से उनकी लॉगिन जानकारी, बैंकिंग डिटेल्स, और अन्य संवेदनशील डेटा चोरी करने की कोशिश करते हैं।

उदाहरण: खिलाड़ी को एक मैसेज या ईमेल प्राप्त होता है जिसमें दावा किया जाता है कि उसका गेमिंग अकाउंट खतरे में है और उसे तुरंत लॉगिन करना चाहिए। इस संदेश में एक फर्जी लिंक दिया होता है। खिलाड़ी जब उस लिंक पर क्लिक करता है और अपनी जानकारी साझा करता है, तो वह जानकारी सीधे स्कैमर्स के हाथों में चली जाती है, जिससे वे खिलाड़ी को आर्थिक और व्यक्तिगत नुकसान पहुंचा सकते हैं।

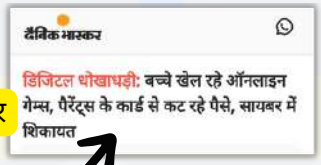
फर्जी इन-गेम आइटम्स और करेंसी

कैसे काम करता है: स्कैमर्स खिलाड़ियों को सस्ते या मुफ्त इन-गेम आइटम्स या करेंसी का लालच देकर उनसे पैसे ऐंठते हैं।



उदाहरण: ऑनलाइन गेम में दुर्लभ आभासी वस्तुओं (जैसे कि **कैरेक्टर्स, स्किन्स, इन-गेम आइटम्स, और करेंसी**) का आकर्षण कई गेमर्स, खासकर बच्चों, के लिए बहुत मजबूत होता है। इस आकर्षण का लाभ उठाकर स्कैमर्स नकली ऑफर्स के जरिए खिलाड़ियों को इन वस्तुओं को सस्ते दामों में खरीदने का लालच देते हैं।

कई बार, बच्चे इन फर्जी ऑफर्स को वास्तविक समझकर अपने माता-पिता के बैंक या क्रेडिट कार्ड का उपयोग करते हैं और कार्ड की डिटेल्स फीड कर देते हैं। जैसे ही ये जानकारी स्कैमर्स के पास पहुंचती है, वे इसे बार-बार इस्तेमाल करके खाते से पैसे निकालते रहते हैं। जब तक माता-पिता को इस बात का एहसास होता है, तब तक उनके बैंक खाते से बड़ी राशि कट चुकी होती है। कुछ मामलों में, स्कैमर्स न केवल पैसे चुराते हैं, बल्कि बैंक अकाउंट की जानकारी से पूरे अकाउंट को भी हैक कर सकते हैं, जिससे और भी गंभीर नुकसान हो सकता है।


दैनिक भास्कर

डिजिटल धोखाधड़ी: बच्चे खेल रहे ऑनलाइन गेम्स, पैरेंट्स के कार्ड से कट रहे पैसे, साइबर में शिकायत

सच्ची घटना पढ़ने के लिए पोस्टर पर क्लिक करें।

खाता अधिग्रहण

Account Take Over (ATO) In Online Gaming

खाता अधिग्रहण (ATO: एटीओ) धोखाधड़ी तब होती है जब एक साइबर अपराधी पीड़ित के लॉगिन क्रेडेंशियल्स तक पहुंच हासिल कर लेता है, जिसका उपयोग वह धन या संवेदनशील जानकारी चुराने के लिए करता है।

- इसमें धोखेबाज एक नकली वेबसाइट तैयार करता है और आकर्षक ऑफर्स (जैसे मुफ्त कैरेक्टर, स्किन्स, हथियार, टोकन, या पॉइंट्स) देने का लालच देता है। जैसे ही खिलाड़ी इस वेबसाइट पर अपने उपयोगकर्ता नाम और पासवर्ड दर्ज करते हैं, उनके गेमिंग अकाउंट का एक्सेस सीधे धोखेबाज के हाथों में चला जाता है।
- धोखेबाज इस तरह आपके गेमिंग अकाउंट का कंट्रोल हासिल करके इसे अन्य व्यक्तियों को बेच देते हैं। अगर आपका क्रेडिट कार्ड विवरण भी सेव है, तो वे इसका भी दुरुपयोग कर सकते हैं, जिससे आपके आर्थिक नुकसान की संभावना बढ़ जाती है।

इसलिए, किसी भी अज्ञात लिंक पर क्लिक करने से बचें और मुफ्त में मिलने वाले ऑफर्स (खासकर गेमिंग की आभासी वस्तुओं के संबंध में) पर भरोसा न करें। आपकी सुरक्षा आपके हाथ में है, सतर्क रहें!


thestatesman.com

The Statesman

Third-party account takeover results in nearly 55% of all fraud in India: Report

Report

पढ़ने के लिए पोस्टर पर क्लिक करें।

- इस तरह की धोखाधड़ी के कारण आपका कोई भी अकाउंट, चाहे वह **सोशल मीडिया, गेमिंग, या बैंकिंग हो**, हैक हो सकता है। इसलिए, सतर्क रहें और अपनी बैंक से संबंधित जानकारी किसी भी थर्ड पार्टी ऐप या अनजान प्लेटफ़ॉर्म पर दर्ज न करें। **आपकी सावधानी ही आपकी सुरक्षा की गारंटी है।**

बाल यौन शोषण (CHILD SEXUAL ABUSE) In Online Gaming

बाल यौन शोषण एक ऐसा गंभीर अपराध है जिसमें बच्चे के साथ यौन गतिविधि या व्यवहार किया जाता है, जो उनकी उम्र, समझ, या सहमति के बिना होता है। ऑनलाइन गेमिंग में **बाल यौन शोषण** एक गंभीर और तेजी से बढ़ती हुई समस्या है। इंटरनेट और डिजिटल प्लेटफार्म्स के व्यापक उपयोग के साथ, बच्चों और किशोरों का ऑनलाइन शोषण करना अपराधियों के लिए आसान हो गया है। इस तरह के मामलों में, अपराधी बच्चों को अश्लील तस्वीरें साझा करने के लिए या बच्चों की **यौन शोषण सामग्री (जैसे तस्वीरें, वीडियो)** का उत्पादन, खरीद, बिक्री या प्रसारण के लिए ऐप्स, वेबसाइट्स, गेम्स, या अन्य डिजिटल तकनीकों का उपयोग करने के लिये उकसाते हैं।

इस प्रकार के शोषण में अक्सर बच्चों का भावनात्मक या शारीरिक फायदा उठाने के लिए उनके साथ जबरदस्ती या धोखे से जुड़ी गतिविधियाँ की जाती हैं। **दुर्व्यवहार के बदले में बच्चों को पैसे, आश्रय जैसी भौतिक वस्तुएँ, या सुरक्षा, स्नेह, और प्यार** जैसी अमूर्त चीजों का वादा या प्रलोभन भी शामिल हो सकता है। यह शोषण बच्चों के मानसिक और शारीरिक स्वास्थ्य पर गहरा प्रभाव डालता है, और इसके दीर्घकालिक परिणाम होते हैं।

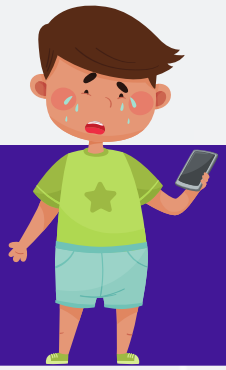
- इसलिए, बच्चों और किशोरों को ऑनलाइन गेमिंग के खतरों के बारे में जागरूक करना अत्यंत आवश्यक है। उन्हें सिखाया जाना चाहिए कि वे ऑनलाइन सुरक्षित व्यवहार कैसे अपनाएं। साथ ही, **माता-पिता और अभिभावकों को बच्चों की ऑनलाइन गतिविधियों पर ध्यान** देना चाहिए और उन्हें ऐसी परिस्थितियों में समर्थन और सुरक्षा प्रदान करने के लिए सही संसाधनों की जानकारी होनी चाहिए।

यह कैसे काम करता है ?

- **ऑनलाइन ग्रूमिंग: एक बढ़ता हुआ खतरा:** ऑनलाइन ग्रूमिंग तब होती है जब एक व्यक्ति (अपराधी) किसी बच्चे का **ऑनलाइन विश्वास जीतने के लिए गलत और भ्रामक तरीकों** का इस्तेमाल करता है, और फिर उस विश्वास का दुरुपयोग करके उसे यौन कृत्य करने के लिए मनाने की कोशिश करता है। यह अपराधी अक्सर सोशल मीडिया, चैट रूम, गेमिंग प्लेटफॉर्म्स, और अन्य डिजिटल माध्यमों का उपयोग करते हैं ताकि बच्चों से दोस्ती कर सकें, उनका विश्वास हासिल कर सकें, और धीरे-धीरे उन्हें अपने जाल में फंसा सकें।
- हालिया रिपोर्ट्स के अनुसार, पिछले **तीन वर्षों में पुलिस द्वारा दर्ज किए गए ऑनलाइन ग्रूमिंग के मामलों की संख्या में 70% की वृद्धि** हुई है। यह आंकड़ा इस बात का स्पष्ट संकेत है कि यह समस्या कितनी गंभीर होती जा रही है। अपराधी अक्सर नकली पहचान का उपयोग करते हैं और बच्चों के साथ व्यक्तिगत जानकारी साझा करने, तस्वीरें भेजने, या वीडियो चैट करने के लिए उन्हें प्रेरित करते हैं। इसके बाद, वे इस जानकारी का इस्तेमाल करके बच्चे को ब्लैकमेल करते हैं या अन्य यौन शोषण गतिविधियों में लिप्त होने के लिए मजबूर करते हैं।

इस बढ़ते खतरे के मद्देनज़र, बच्चों को इंटरनेट के सुरक्षित उपयोग के बारे में जागरूक करना और उन्हें ऑनलाइन बातचीत में सतर्क रहने की शिक्षा देना बहुत जरूरी है। माता-पिता और अभिभावकों को भी बच्चों की ऑनलाइन गतिविधियों पर नजर रखनी चाहिए और किसी भी संदिग्ध गतिविधि के प्रति सजग रहना चाहिए।

Source: Gaming And The Metaverse (Bracket Foundation).pdf



बाल यौन शोषण सामग्री (CHILD SEXUAL ABUSE/EXPLOITATION MATERIAL:CSAM)

In online Gaming

Child Sexual Abuse Material

ऑनलाइन बाल यौन शोषण सामग्री **(Child Sexual Abuse/exploitation Material:CSAM)** का मतलब उन सामग्रियों से है, जो बच्चों के यौन शोषण को दर्शाती हैं। **"बाल पोर्नोग्राफी"** शब्द को अंतरराष्ट्रीय संगठनों ने अस्वीकार कर इसे **"बाल यौन शोषण सामग्री"** कहा है, ताकि इस गंभीर अपराध की प्रकृति को स्पष्ट किया जा सके।

संचालन के तरीके:

- **डिजिटल प्लेटफॉर्म्स पर प्रसार:** CSAM को ईमेल, इंस्टेंट मैसेजिंग, चैट रूम, और सोशल मीडिया के माध्यम से साझा किया जाता है।
- **डार्कनेट का उपयोग:** अपराधी डार्कनेट (इंटरनेट का गुप्त हिस्सा) पर ऐसी सामग्री को छिपाकर रखते हैं और एन्क्रिप्शन का उपयोग कर कानून प्रवर्तन से बचने की कोशिश करते हैं।
- **पासवर्ड-प्रोटेक्टेड साइट्स और फोरम्स:** विशेष साइट्स और फोरम्स पर सदस्यता के लिए अश्लील सामग्री अपलोड करने की शर्त होती है।

AI द्वारा निर्मित यौन दुर्व्यवहार की तस्वीरें (AI-GENERATED SEXUAL ABUSE IMAGERY)

AI Genetrated Image

जेनरेटिव AI डिजिटल दुनिया में क्रांति ला रहा है। पारंपरिक AI सिस्टम, जो पैटर्न की पहचान और पूर्वानुमान लगाते हैं, की तुलना में जेनरेटिव AI नई सामग्री जैसे टेक्स्ट, चित्र और ऑडियो आदि बनाता है।

अपराधी जेनरेटिव AI का उपयोग नकली या वास्तविक दिखने वाली अश्लील सामग्री (CSAM) तैयार करके बच्चों का यौन शोषण कर रहे हैं। ऐसे मामलों में वृद्धि हो रही है, जिससे बच्चों के खिलाफ होने वाले अपराधों का खतरा और बढ़ गया है।

जागरूकता और सुरक्षा उपायों की आवश्यकता है ताकि इस तकनीक के दुरुपयोग को रोका जा सके।

फर्जी प्रोफाइल बनाकर (BY CREATING FAKE PROFILE)

In Online Gaming

By Creating Fake Profile

- अपराधी अक्सर बच्चों को निशाना बनाने के लिए फर्जी प्रोफाइल बनाते हैं। सोशल नेटवर्क के अनुमान के अनुसार, **मासिक सक्रिय उपयोगकर्ताओं में से लगभग 11% डुप्लिकेट खाते** होते हैं, जो करीब **275 मिलियन फर्जी प्रोफाइल्स** के बराबर हैं।
- ये नकली प्रोफाइल बच्चों को धोखा देने और उनका शोषण करने के लिए बनाई जाती हैं, जिससे वे आसानी से अपराधियों के जाल में फंस सकते हैं।

फर्जी गेम ऐप/वेबसाइट

By Whatsapp + Telegram

वर्तमान में, फर्जी गेम ऐप्स और वेबसाइट्स का उपयोग करके ठग लोगों को धोखा दे रहे हैं। ये स्कैम ऐसे लोगों को लक्षित करते हैं जो गेम खेलकर पैसे कमाना चाहते हैं।

कैसे काम करता है-

- **लुभावने ऑफ़र:** ठग टेलिग्राम चैनल या ग्रुप बनाते हैं, जहां वे आकर्षक गेम ऑफर्स और 100% जीत की गारंटी के साथ बेटिंग का प्रलोभन देते हैं।
- **फर्जी वेबसाइट पर रीडायरेक्ट:** व्हाट्सएप लिंक पर क्लिक करने पर एक फर्जी वेबसाइट पर ले जाया जाता है, जहां "उच्च रिटर्न" का वादा किया जाता है।
- **धोखाधड़ी का जाल:** एक बार भुगतान करने के बाद, वे नकली गेमिंग वेबसाइट पर आपको दिखाते हैं कि आपके द्वारा भुगतान की गई राशि के बदले में बड़ी रकम प्राप्त होने वाली है, लेकिन जब आप इसे निकालने का प्रयास करते हैं, तो वे फिर से पैसे मांगते हैं, यह कहकर कि इससे आपकी जमा राशि और रिटर्न एक साथ रिलीज़ होंगे।

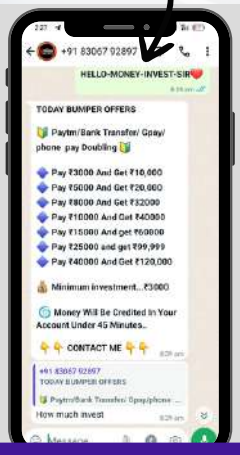
सच्ची घटना -

पढ़ने के लिए पोस्टर पर क्लिक करें।

- **निरंतर ठगी:** यह प्रक्रिया तब तक चलती रहती है जब तक कि आप ठगी का शिकार नहीं बन जाते।

इसलिए विश्वसनीय स्रोतों से ही ऐप्स और गेम डाउनलोड करें और अज्ञात व्यक्तियों के साथ वित्तीय जानकारी साझा न करें।

कभी भी टेलीग्राम/व्हाट्सएप के माध्यम से दिखाए जाने वाले ऐसे ऑफर या थर्ड पार्टी वेबसाइट/ऐप पर भरोसा न करे।



लाइव स्ट्रीमिंग के माध्यम से बाल यौन शोषण

In Online Gaming

ऑनलाइन गेम्स में लाइव स्ट्रीमिंग का उपयोग करके अपराधी बच्चों का शोषण करते हैं। वे नकली प्रोफाइल बनाकर या चैट के माध्यम से बच्चों से संपर्क करते हैं और उन्हें विभिन्न तरीकों से धोखा देकर अश्लील सामग्री साझा करने के लिए मजबूर करते हैं। इसके बाद, इन अश्लील सामग्रियों का उपयोग कर बच्चों को ब्लैकमेल किया जाता है या इंटरनेट पर वितरित किया जाता है।

- इस प्रकार के स्कैम से बचने के लिए, बच्चों को ऑनलाइन सुरक्षा के बारे में जागरूक करना और उनकी ऑनलाइन गतिविधियों पर नजर रखना जरूरी है।

ऑनलाइन गेमिंग में धर्म परिवर्तन से जुड़े खतरे

- हाल ही में यह सामने आया है कि कुछ ऑनलाइन गेमिंग प्लेटफॉर्म का इस्तेमाल **बच्चों को धर्म परिवर्तन** के लिए प्रलोभित करने में किया जा रहा है।
- ये अपराधी गेम्स के जरिए बच्चों से दोस्ती करते हैं और फिर चैट ऐप्स पर उन्हें प्रलोभन देते हैं। धीरे-धीरे, वे अपने विचारधारा को बच्चों पर थोपने की कोशिश करते हैं, जिससे बच्चे मानसिक रूप से प्रभावित होते हैं।

ये कैसे काम करता है -

सच्ची घटना -

पढ़ने के लिए पोस्टर पर क्लिक करें।

- **पहला चरण:** अपराधी फर्जी प्रोफाइल बनाकर बच्चों को गेम जैसे 'Fortnite' में शामिल करते हैं। गेम हारने पर उन्हें नमाज की आयतें पढ़ने के लिए उकसाया जाता है, जिससे बच्चे जीतने लगते हैं और इस्लाम की ओर आकर्षित होते हैं।
- **दूसरा चरण:** "Discord" ऐप पर चैटिंग के जरिए बच्चों का विश्वास जीतकर उन्हें इस्लाम के फायदे बताते हैं और धार्मिक वीडियो दिखाते हैं।
- **तीसरा चरण:** बच्चों से एफिडेविट पर हस्ताक्षर कराए जाते हैं, जिसमें लिखा होता है कि वे अपनी मर्जी से धर्म परिवर्तन कर रहे हैं।

यह घोटाला बच्चों के मानसिक और भावनात्मक शोषण के माध्यम से उन्हें धोखे से धर्म परिवर्तन के लिए प्रेरित करता है।

ऐसे घोटालों से बचने के लिए अभिभावकों को अपने बच्चों की ऑनलाइन गतिविधियों पर नजर रखनी चाहिए, उन्हें जागरूक करना चाहिए, और अनजान लोगों से बातचीत करने से रोकना चाहिए।

कार्य-प्रणाली एवं सुरक्षा सावधानियां

अपराधियों की रणनीतियाँ:

- **नकली प्रोफाइल बनाना:** अपराधी नकली प्रोफाइल (आकर्षक लड़की या लड़के की तस्वीर और नाम बदलकर) बनाते हैं और बच्चों से दोस्ती करने का प्रयास करते हैं।
- **भावनात्मक रूप से जोड़ना:** विश्वास जीतकर अश्लील चैट और सामग्री साझा करते हैं।
- **ब्लैकमेल करना:** बच्चों को अनुचित हरकतें करने के लिए मजबूर करते हैं और उनकी सामग्री का दुरुपयोग करके ब्लैकमेल करते हैं।

रोकथाम के उपाय:

- **जागरूकता और शिक्षा:** बच्चों को ऑनलाइन सुरक्षा के बारे में जागरूक करें और उन्हें अनजान प्रोफाइल्स से बचने के लिए शिक्षित करें।
- **पेरेंटल कंट्रोल्स:** बच्चों की ऑनलाइन गतिविधियों की निगरानी के लिए पेरेंटल कंट्रोल्स का उपयोग करें।
- **रिपोर्टिंग:** संदिग्ध गतिविधियों की तुरंत रिपोर्ट करें। इस तरह की सतर्कता से बच्चों को सुरक्षित रखा जा सकता है और अपराधियों के मंसूबों को नाकाम किया जा सकता है।

सच्ची घटना के माध्यम से फ्रॉड को समझना

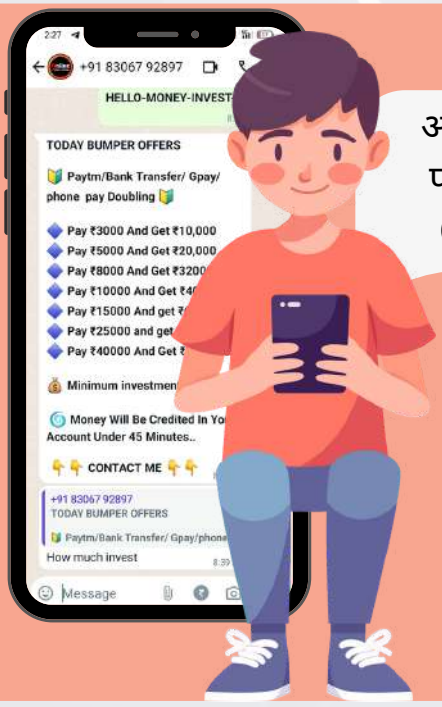
यह घटना नालासोपारा के एक 18 वर्षीय छात्र की है, जिसने 2 लाख रुपये की साइबर धोखाधड़ी का शिकार होने के बाद दुखद रूप से आत्महत्या कर ली। इस घटना से यह स्पष्ट होता है कि बच्चों को साइबर अपराधों के प्रति जागरूक करना अत्यंत आवश्यक है। आइए समझते है बच्चे ने क्या गलती की और आप अपने बच्चे को इससे कैसे बचा सकते है।

पढ़ने के लिए पोस्टर पर क्लिक करें।

मोहन (बदला हुआ नाम) अपनी मां के फोन में हर दिन की भांति आज भी गेम खेल रहा है।

गेम खेलने के दौरान अचानक मोबाइल पर एक संदेश आता है।

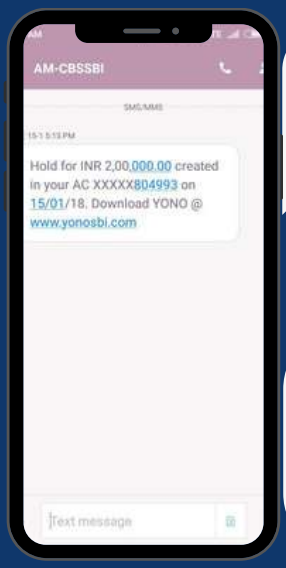
संदेश गेम के कुछ आकर्षक ऑफर के बारे में होता है जिसे क्लेम करने के लिए नीचे लिंक दिया गया होता है।



आर्कषक ऑफर पढ़ते ही मोहन उस लिंक पर क्लिक कर देता है, और खुले पेज पर OTP के लिए अनुरोध किया जाता है ।

अब मोबाइल पर आई ओटीपी मोहन उस पेज में दर्ज करता है।

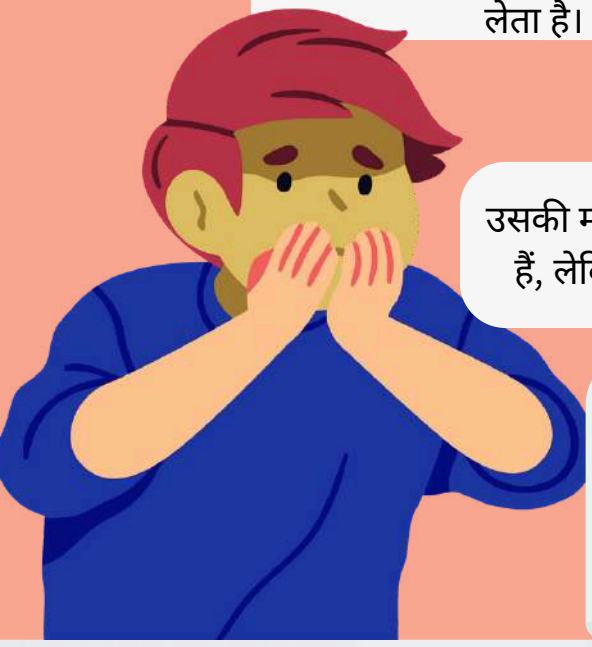
थोड़ी ही देर बाद मोबाईल पर एक संदेश आता है जिसे देख मोहन डर जाता है।



आपके A/C **** से 200000(2 लाख) रुपए डेबिट हो गए हैं।

मोहन घबराहट से भर जाता है, उसे समझ नहीं आ रहा कि क्या करे। उसके मन में यह डर बैठ जाता है कि उसके पिता नाराज़ होंगे, क्योंकि उसने उनकी मेहनत की कमाई गँवा दी है। वह चिंता और तनाव में डूब जाता है, सोचते हुए कि अब आगे क्या होगा।

मोहन घबराहट में घर में रखी पेस्टीसाइड (जहरीला रसायन) की बोतल उठाकर पी लेता है।



उसकी मां उसे तुरंत अस्पताल ले जाती हैं, लेकिन मोहन नहीं बच पाता हैं।

- यह घटना इस बात की ओर इशारा करती है कि साइबर धोखाधड़ी के मामलों में जागरूकता और बच्चों को भावनात्मक समर्थन देना कितना महत्वपूर्ण है, ताकि वे कठिन परिस्थितियों में सही निर्णय ले सकें।
- माता-पिता और अभिभावकों को बच्चों के साथ संवाद बनाए रखना चाहिए और उनकी चिंताओं को गंभीरता से लेना चाहिए साथ ही ऑनलाइन गेमिंग और सोशल मीडिया प्लेटफॉर्म्स पर उनकी गतिविधियों की निगरानी रखें।
- बच्चों को दी हुई मोबाइल फोन में पैरेंटल कंट्रोल अवश्य लगाएं।

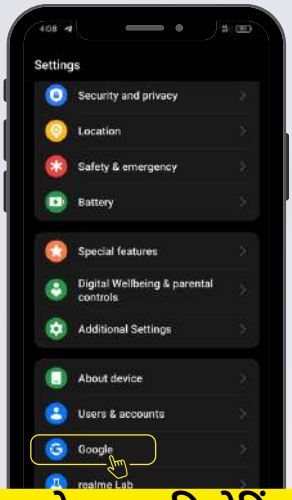
साइबर सुरक्षा टिप्स - 1

पैरेंटल कंट्रोल एक्टिवेट करें।

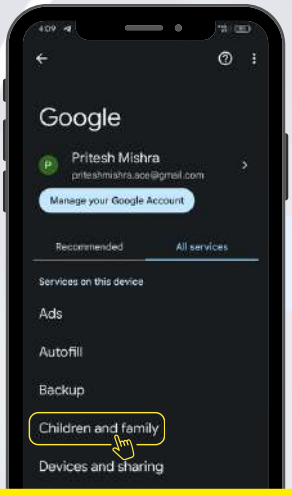
पैरेंटल कंट्रोल एक ऐसी तकनीक या सॉफ़्टवेयर है जिसका उपयोग माता-पिता द्वारा अपने बच्चों की ऑनलाइन गतिविधियों की निगरानी और नियंत्रण के लिए किया जाता है।

इसे एक्टिवेट करने के लिए आपको 2 मोबाइल फ़ोन की जरुरत होगी पहली पेरेंट्स की और दूसरी बच्चे की।

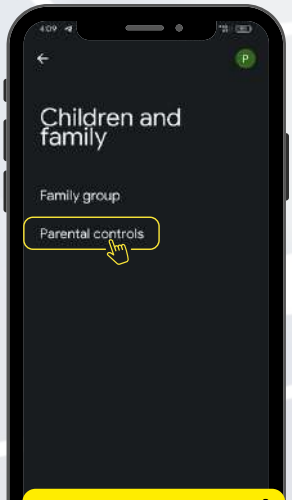
पेरेंट्स के फ़ोन में सबसे पहले -



1-मोबाइल की सेटिंग खोले और Google पर क्लिक करें ।

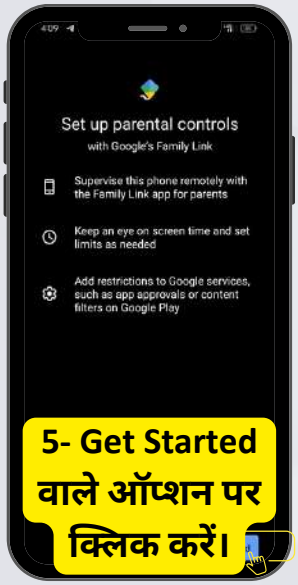


2- अब Children/child / kids and Family पर क्लिक करें ।

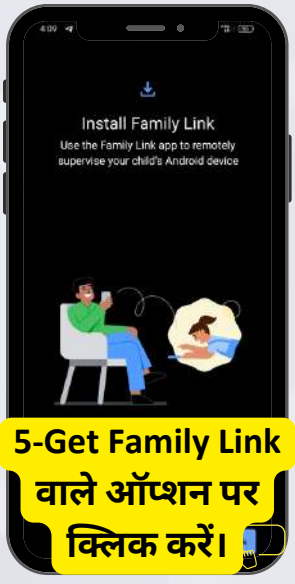


3- अब parental Controls वाले ऑप्शन पर क्लिक करें।

4- Parent वाले ऑप्शन पर क्लिक करें।

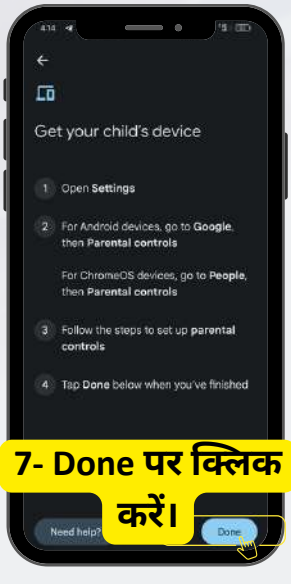


5- Get Started वाले ऑप्शन पर क्लिक करें।



5-Get Family Link वाले ऑप्शन पर क्लिक करें।

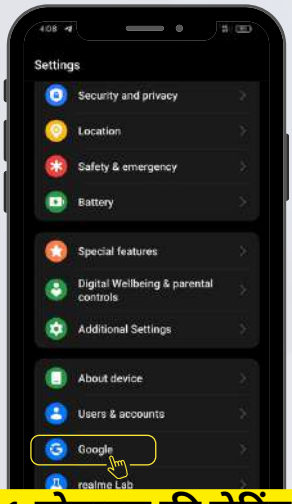
6-अब इस ऐप को इंस्टाल करे और ओपन कर अपने इमेल से लॉगिन करे।



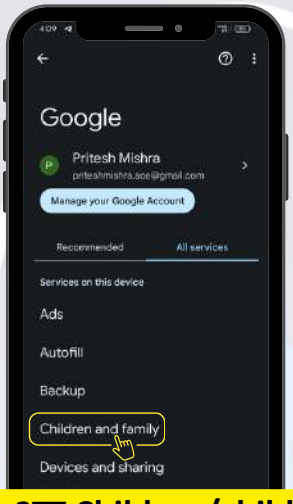
7- Done पर क्लिक करें।

Smart Parents

अब बच्चे के फ़ोन में सबसे पहले -



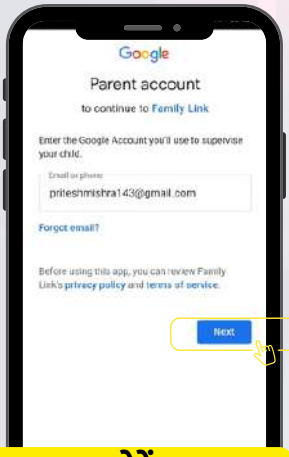
1-मोबाइल की सेटिंग खोले और Google पर क्लिक करें ।



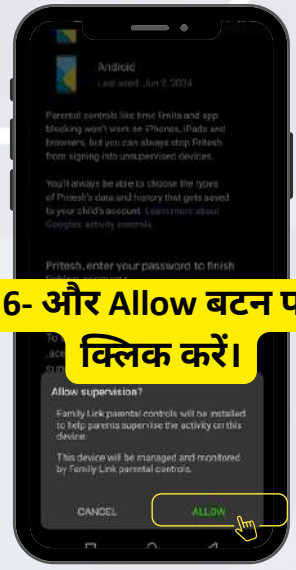
2- अब Children/child / kids and Family पर क्लिक करें ।

3- अब parental Controls वाले ऑप्शन पर क्लिक करें।

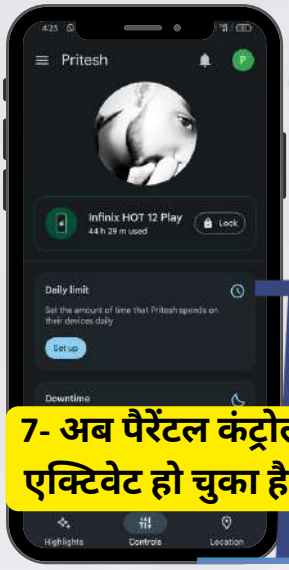
4- child or teenager वाले ऑप्शन पर क्लिक करें।



5- अब पेरेंट अपना Gmail और पासवर्ड यहां दर्ज करें ।



6- और Allow बटन पर क्लिक करें।



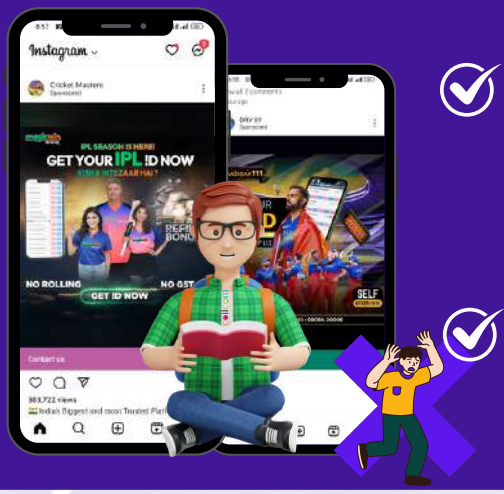
7- अब पैरेंटल कंट्रोल एक्टिवेट हो चुका है।

अब आप अपने बच्चों की ऑनलाइन गतिविधियों पर नियंत्रण रख सकते हैं, जैसे कि अगर वे कोई गेम अधिक खेलते हैं, तो आप उस गेम पर समय सीमा निर्धारित कर सकते हैं या ऐप को ब्लॉक कर सकते हैं।

इस प्रकार, आप एक स्मार्ट पेरेंट बनकर उनके स्क्रीन टाइम को मैनेज कर सकते हैं और उनके भविष्य को सुरक्षित बना सकते हैं।

साइबर सुरक्षा टिप्स - 2

सोशल मीडिया पर इस तरह के गेमिंग ऐप के ad दिखाई दे तो वहाँ अपनी व्यक्तिगत जानकारी जैसे नाम, पता व मोबाईल नंबर इत्यादि शेयर न करें।



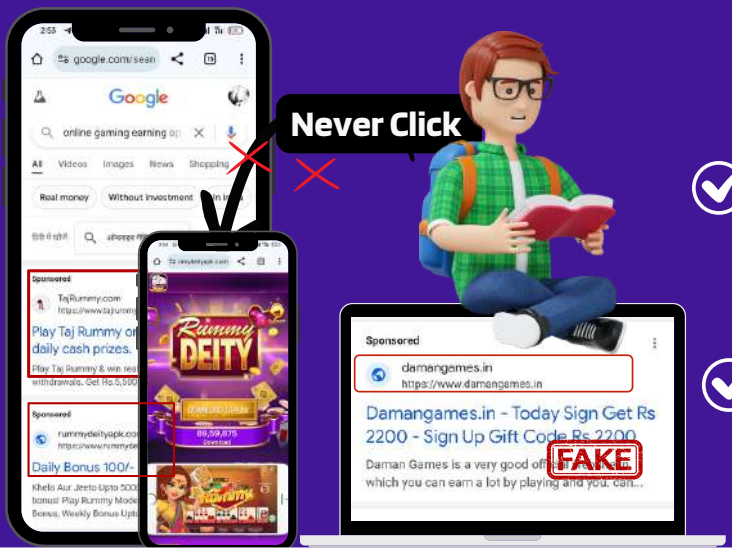
ध्यान रखें -

HELPFUL TIPS

- ऐसे Ad पर अपनी प्रतिक्रिया न दे, कोई भी निजी जानकारी शेयर न करें, और सोशल मीडिया पर यूजर के द्वारा दिए गए कमेंट की प्रतिक्रिया पर भी कभी विश्वास न करें।
- स्कैम से बचने के लिए व गेमिंग ऐप डाउनलोड करने के लिए हमेशा गूगल प्ले स्टोर या एप्पल स्टोर से ही डाउनलोड करें।

साइबर सुरक्षा टिप्स - 3

गूगल सर्च के परिणामों पर बिना सोचे-समझे भरोसा न करें।



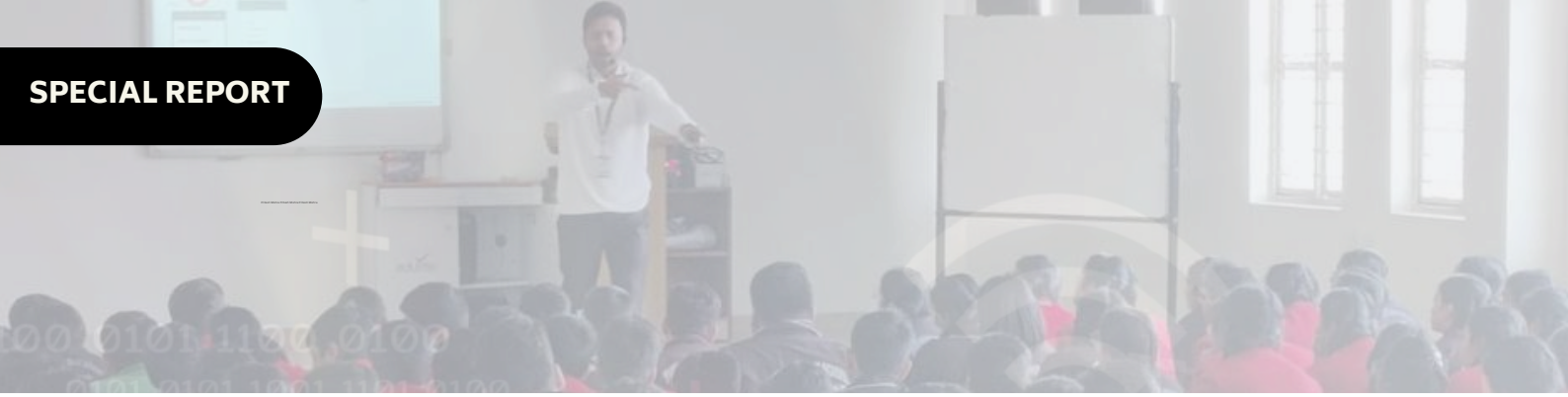
ध्यान रखें -

HELPFUL TIPS

- गूगल सर्च पर दिखने वाले परिणाम अगर स्पॉन्सर्ड है तो क्लिक करने से बचे।
- गूगल सर्च परिणाम पर क्लिक करते समय उस वेबसाइट की प्रमाणिकता को जरूर जाँच ले।

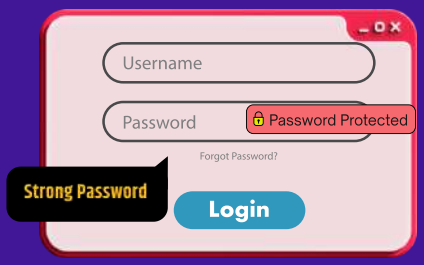
साइबर सुरक्षा टिप्स - 4

Bank details जैसे OTP, CVV, customer ID, UPI pin इत्यादि किसी भी गेमिंग वेबसाइट पर सांझा / सेव न करें।



साइबर सुरक्षा टिप्स - 5

अपने कार्ड की जानकारी को सुरक्षित रखे, इसके लिए एक अच्छा पासवर्ड चुनें और इसे नियमित रूप से बदलते रहें।

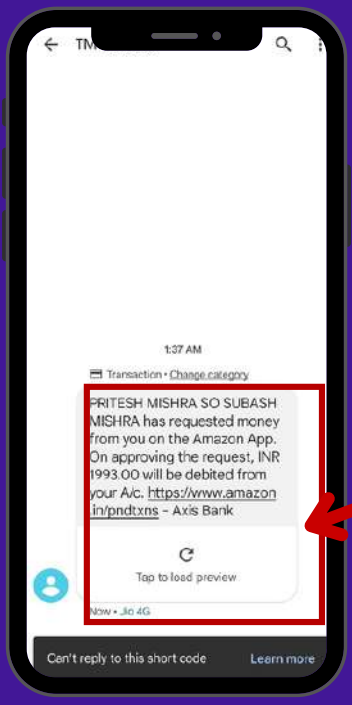


अपने ऑनलाइन खातों के लिए मजबूत पासवर्ड उपयोग करें और कई खातों पर एक ही पासवर्ड का उपयोग न करें।
Ex- Xyz#243@

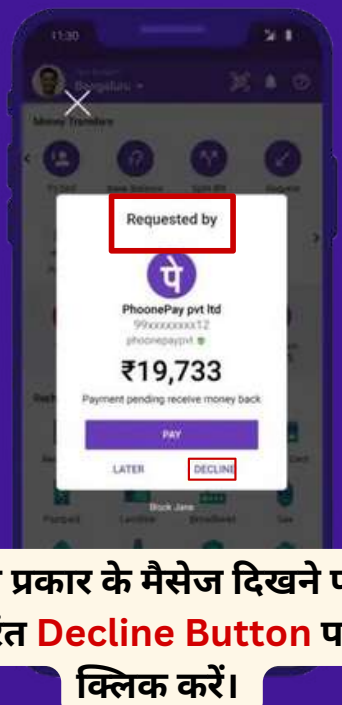
साइबर सुरक्षा टिप्स - 6

पैसे रिसीव करने के लिए यदि कोई लिंक भेजे तो उसपर भूलकर भी क्लिक ना करें, और ध्यान रहे कभी भी पैसे लेने के लिए हमे UPI Pin या OTP शेयर करने की आवश्यकता नही होती है।

UPI पिन और OTP सिर्फ पैसे ट्रांसफर करने के लिए जरूरत होती है। एक गलत कदम लेने से पैसे लेने कि वजाय हमे देने पड़ जायेंगे।



इस तरह के लिंक को भूलकर भी क्लिक ना करें



इस प्रकार के मैसेज दिखने पर तुरंत Decline Button पर क्लिक करें।

फ्रॉड होने की स्थिति में क्या करें ?

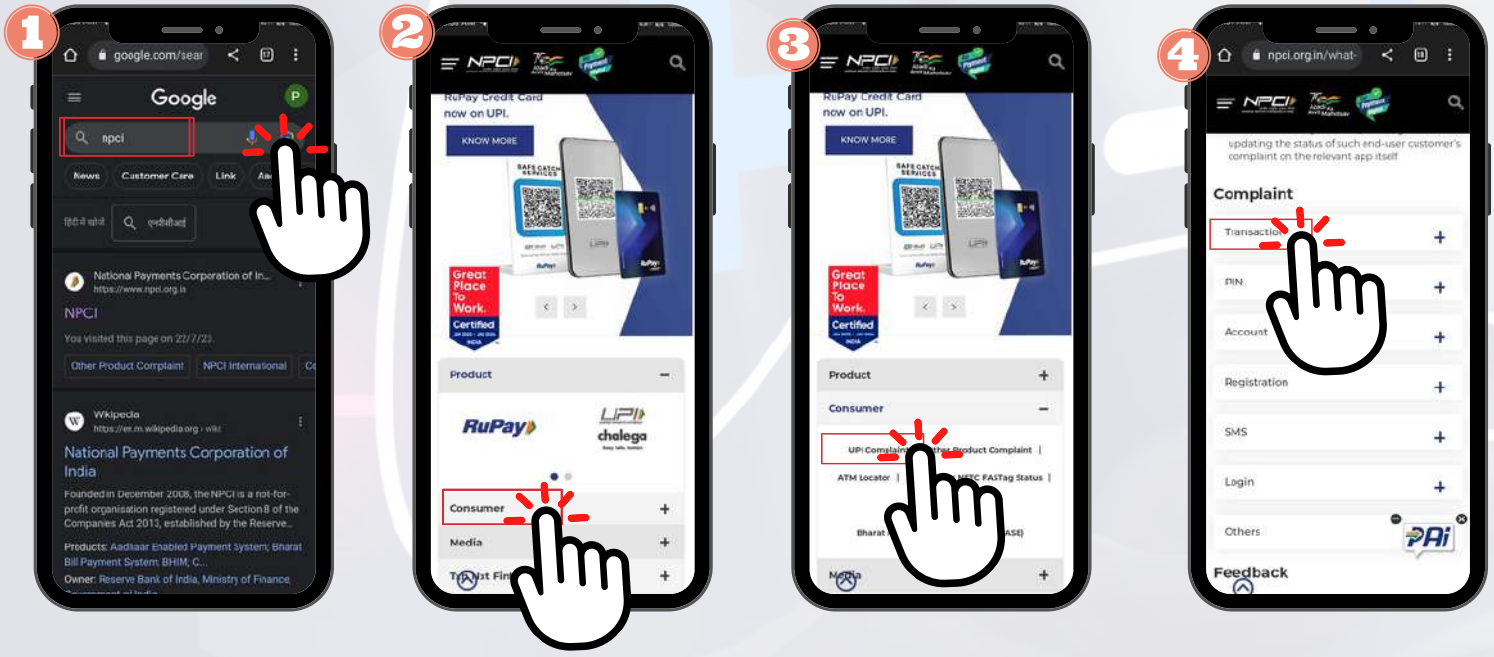
यदि आप इस तरह के फ्रॉड के शिकार हो जाते है तो तुरंत ही आप सभी chat, भेजे गए डॉक्यूमेंट, और भेजे गए पैसों के स्क्रीन शॉट के साथ www.cybercrime.gov.in or 1930 पर संपर्क कर अपनी शिकायत दर्ज करें । ऑनलाइन शिकायत करने के बाद हमे पुलिस स्टेशन जाकर दुबारा शिकायत दर्ज करवाने की जरूरत नहीं होती हैं।

शिकायत दर्ज करने के लिए यहाँ क्लिक करें और आगे के चरण का अनुसरण कर अपनी शिकायत दर्ज करें ।

ध्यान रखें - किसी भी तरह का ऑनलाइन फ्रॉड होने पर हमे डरे बिना ऑनलाइन शिकायत जरूर दर्ज करवानी चाहिए।

फ्रॉड होने की स्थिति में क्या करें ?

UPI के माध्यम से यदि फ्रॉड हो या गलती से किसी अन्य के UPI पर पैसे चले जाए तो उस स्थिति में हम विभिन्न चरणों का पालन कर अपने पैसे पुनः प्राप्त कर सकते हैं।



Step 1- गूगल पर NPCI लिखकर सर्च करे, अथवा वेबसाइट www.npci.org.in पर क्लिक करें।

Step 2- अब आप NPCI की होम पेज पर है, नीचे स्क्रॉल करे और consumer पर क्लिक करें।

Step 3- अब UPI पर क्लिक करें।

Step 4- नीचे स्क्रॉल करे और complaint के अंतर्गत Transaction वाले ऑप्शन पर क्लिक करें ।

Step 5- अपने समस्या के अनुसार विवरण भरे । और सबमिट बटन पर क्लिक करें।

* शिकायत विलम्ब से होने की स्थिति में पैसा वापस मिलना मुश्किल हो सकता है।

फ्रॉड होने की स्थिति में क्या करें ?

आप अपने शहर के **नजदीकी साइबर सेल** में भी अपनी शिकायत दर्ज कर सकते है ताकि आपको जल्द से जल्द समाधान मिल सके।

उत्तर प्रदेश पुलिस के साइबर थानों के मोबाइल नम्बर एवं ईमेल

CLICK HERE

Delhi District Cyber Cells CLICK HERE

नि:शुल्क ऑनलाइन साइबर प्रशिक्षण

आजकल इसी प्रकार से अनेकों साइबर अपराध तेजी से प्रसारित हो रहे, जिसे देखते हुए हमने आपके लिए बिल्कुल फ्री में साइबर प्रशिक्षण महा-अभियान चलाया है जिसमे आप ऐसे साइबर अपराध से बचने के तरीको के बारे में सीख पाएंगे।

इस प्रशिक्षण में स्कैम को समझाने के लिए कहानी और छोटे-छोटे वीडियो का भी इस्तेमाल किया गया है, इसे इंग्लिश और हिंदी दोनों भाषा में तैयार किया गया, लगभग 30 मिनट्स का समय इसे पूरा करने में लगता है, और अंत में एक प्रमाण पत्र स्कोर कार्ड का साथ दिया जाता है।

इस प्रशिक्षण को एक बार जरूर करें।

- हिंदी में साइबर प्रशिक्षण- https://forms.gle/AJajaozGwTjLPExC7
- Cyber Training in English- https://forms.gle/8LyAQPWPucn8LHir8

संस्थापक के बारे में

DR GAURAV KUMAR

(Founder and Director of CollCom, Asst Prof at Bennett University, Greater Noida)

डॉ गौरव वर्तमान में बेनेट विश्वविद्यालय (टाइम्स ग्रुप), ग्रेटर नॉएडा, उत्तर प्रदेश में कंप्यूटर इंजीनियरिंग विभाग में सहायक प्रोफेसर के पद पर कार्यरत हैं । वह एक सामाजिक उद्यमी और CollCom (कॉलेज कम्युनिटी सोशल वेंचर) के संस्थापक और राष्ट्रीय सेवा योजना बेनेट विश्वविद्यालय के कार्यक्रम अधिकारी भी है। डॉ कुमार हमारे देश के प्रतिष्ठित संस्थानों में से एक जवाहरलाल नेहरू विश्वविद्यालय, नई दिल्ली से कंप्यूटर विज्ञान में एम.टेक और पीएचडी पूरी की है। अपनी शिक्षा के दौरान, वह सामाजिक गतिविधियों में काफी सक्रिय थे जैसे स्लम बस्ती में बच्चों को पढ़ाना, Waste मैनेजमेंट, वृक्षारोपण अभियान, रक्त दान, स्वास्थ्य, योग और फिटनेस के लिए सभी को जागरूक करना जैसे विषय पर काफी काम किया है ।

उनके इस अथक प्रयास के लिए उन्हें विश्वविद्यालय से स्वर्ण पदक पुरस्कार और मानव संसाधन विकास मंत्रालय, भारत सरकार से सर्वश्रेष्ठ स्वयंसेवी (बेस्ट वालंटियर अवार्ड) का पुरस्कार से भी सम्मानित किया गया है। कोविड के समय में डॉ कुमार शांत नहीं बैठे । उन्होंने प्लाज्मा और ऑक्सीजन सपोर्ट के लिए लोगों की मदद करने का काम शुरू किया। उन्होंने देखा की हर व्यक्ति, बच्चे से लेकर बूढ़े तक, सभी लोग अपने दैनिक कार्य करने के लिए इंटरनेट पर निर्भर होते जा रहे है। जल्द ही, उन्हें इंटरनेट की दुनिया में तेजी से बढ़ रहे साइबर अपराध के बारे में जागरूकता की कमी के महत्व का एहसास हुआ। उन्होंने साइबर अपराध जागरूकता पर एक मेगा अभियान शुरू किया। उन्होंने विभिन्न स्कूलों और कॉलेजों (ऑफ़लाइन और ऑनलाइन) का दौरा करना शुरू किया और साइबर अपराध जागरूकता पर 35 से अधिक कार्यशालाएँ की । उन्होंने एक छोटा और बहुत ही अभिनव ऑनलाइन सेल्फ गाइड साइबर क्राइम अवेयरनेस ट्रेनिंग मॉड्यूल विकसित किया, जिसमें अभी तक **75,000** से अधिक लोगों ने भाग लिया और लाभान्वित हुए ।

उनका लक्ष्य अगले दो वर्षों में हमारे देश के 10 लाख लोगों को इंटरनेट की दुनिया में सशक्त बनाना है।

संपादक के संदेश..

MR. PRITESH MISHRA

(National Coordinator, CollCom)

किसी व्यक्ति के साथ फ्रॉड होने का अर्थ ये कदापि नहीं है की वो शिक्षित नहीं है, केवल सीधा सा अर्थ है वो उस बात से अनभिज्ञ/जागरूक नही था । अतः फ्रॉड होने के स्थिति में आप सबसे पहले ज़रा भी न घबराए, परिवार वाले डाटेंगे या मित्र क्या कहेंगे ? ये कदापि न सोचे या कोई भी गलत फैसला न ले, समय रहते यदि आप शिकायत दर्ज करवा देते है तो आपके पैसे मिलने के अवसर बढ़ जाते है ।

अब तो RBI के दिशा निर्देश के अनुसार आप फ्रॉड होने के तुरंत बाद यदि अपने संबंधित बैंक में शिकायत दर्ज कराते है तो वो 90 दिन के भीतर ही आपकी समस्या सुलझाने का प्रयास करते है। परंतु आप को यहां तक पहुंचने की आवश्यकता ही क्या है, बस थोड़ी सी सावधानी के साथ आप अपने और अपने से संबंधित लोगों को साइबर अपराध से बचा सकते हैं ।

वर्तमान समय और भी भयावह है इस बढ़ती तकनीक में ठग आपके थोड़ी सी जानकारी से आपके पूरे जीवन को संकट में डाल सकते है, आने वाले समय में **कॉल स्पूफिंग के खतरे अधिक है** जिसमे आपको अपने संबंधी के मोबाइल में सेव नंबर से उन्ही के आवाज में कॉल आयेगा परंतु वो ठग होगा। इससे बचने के लिए हर एक चीज को सत्यापित करे बिना किसी के बात में न आए और अपनी व्यक्तिगत जानकारियों को ऑनलाइन कम से कम अपडेट करे।

समय-समय पर आपको साइबर से संबंधित जानकारी हम अपने ऑफिशियल वेबसाइट/ सोशल मीडिया/यूट्यूब वीडियो के माध्यम से साझा करते रहेगें ।

जागरूक रहें, सुरक्षित रहें !

सलाहकार सदस्य

Dr Anil Kumar Singh
(Asst. Professor, Jawaharlal Nehru University)

Shri Anshumali Sharma
(Ex-State Liaison Officer (SLO) NSS, Uttar Pradesh)

Dr. Sanjeev Sharma
(Associate Professor, JNU, New Delhi)

Shri Gautam Kumar
(Executive Engineer, WRD, Govt of Bihar)

Shri Amrish Kumar Niranjan
(Youth Assistant, NSS, Delhi)

Shri Sintoo Kumar
(TGT Teacher, Govt of Delhi)

Shri OP Mishra
(Entrepreneur and Director of Jetex Infotech)

Shri Ranjan Kumar
(Senior Product Manager, Microsoft)

कार्यकारी सदस्य

Dr Gaurav Kumar
(Asst Prof, Bennett University, Founder CollCom)

Mr Priteesh Kumar
(Asst. Director-Collaboration, CollCom)

Shri Satya Mishra
(Asst. Director-Marketing, CollCom)

Mr Pritesh Mishra
(National Coordinator, CollCom)

Mr Sumit Kumar
(State Coordinator, CollCom)

Ms Shweta Kumari
(Social Media Head, CollCom)

WWW.COLLCOM.ORG

मैगज़ीन के पिछले संस्करण

March,2024

FEB, 2024

JAN, 2024

Dec, 2023

NOV, 2023

Oct,2023

Sept,2023

Aug,2023

July,2023

June,2023

May,2023

April,2023

March,2023

FEB,2023

JAN,2023

DEC,2022

किसी भी मैगजीन को पढ़ने के लिए उस मैगजीन पर क्लिक करें।

पढ़ने के बाद अपना सुझाव अवश्य दें। https://g.page/r/CZmEUz-HXMe0EAI/review

collcom
Empowering Youth through Community Service

सावधान रहें, सुरक्षित रहें!

अपने मित्रों व रिश्तेदारों के साथ इस मैगज़ीन को शेयर जरूर करें ।

हमसे लगातार साइबर अपडेट्स पाने के लिए इस QR कोड को स्कैन करें और हमारे आधिकारिक चैनल/ग्रुप को सब्सक्राइब करें।

SUBSCRIBE

Cyber Sanskar
WhatsApp Channel

Telegram

Click to Check Out some interesting video on YouTube
https://www.youtube.com/@collcom

For volunteering, Type **Join** and Send it on **WhatsApp +91-9868189955**